Declassified and Approved For Release 2013/03/04 : CIA-RDP91B00060R000100320006-4 67X-88

LOGGED
26 JUN 1988

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

MAY 26 1988

DDA/REG
LOGGED

MEMORANDUM FOR SENIOR INFORMATION RESOURCE MANAGEMENT OFFICIALS

FROM: James B. MacRae, Jr.
Acting Administrator and
Deputy Administrator
Office of Information and
Regulatory Affairs

SUBJECT: Request for Comment on Draft Guidance for the Submission of Computer System Security Plans Required by the Computer Security Act of 1987

As you may know, the Computer Security Act of 1987 (P.L. 100-235) requires agencies to:

- identify Federal computer systems[1] that contain sensitive information by July 8, 1988;

- establish a security plan for the security of each such computer system by January 8, 1989 that is commensurate with the risk and magnitude of the harm resulting from loss, misuse, or unauthorized access to or modification of the information contained in such system; and

- send copies of such plans to the National Bureau of Standards (NBS) and the National Security Agency (NSA) for advice and comment. Plans are subject to disapproval by the Office of Management and Budget (OMB).

Agencies are also required to provide for mandatory periodic training in computer security awareness and accepted computer security practice for all employees involved in the management, use or operation of Federal computer systems. Such training is to be provided in accordance with guidelines developed by NBS and, for Federal civilian employees, in accordance with regulations to be issued by the Office of Personnel Management (OPM). Training must be started within 60 days of the issuance of the OPM regulations.

Attached for comment is a draft of guidance for the preparation and submission of security plans prepared by NBS, NSA and OMB staff. In view of the deadlines set in the statute, our intent is to issue such guidance as an OMB Bulletin by early July. Therefore, we need any comments/suggestions by June 10. Ed Springer of my staff (395-4814) is available to answer any questions concerning the draft.

Thank you for your prompt attention to this request.

Attachment

[1] Federal computer systems include systems operated by contractors or other organizations on behalf of the Federal government to accomplish a Federal function.

Declassified and Approved For Release 2013/03/04 : CIA-RDP91B00060R000100320006-4

------ DRAFT ------
Revised: May 25, 1988

GUIDANCE FOR PREPARATION AND SUBMISSION OF SECURITY PLANS FOR FEDERAL COMPUTER SYSTEMS CONTAINING SENSITIVE INFORMATION

PURPOSE

The purpose of this guidance is to provide agencies with information needed to prepare and submit computer security plans in accordance with the Computer Security Act of 1987.

AUTHORITY

The Computer Security Act of 1987 (P.L. 100-235) requires Federal agencies to identify computer systems containing sensitive information and to prepare a plan to ensure the security and privacy of each such system. The Act further requires that agencies submit their security plans to NBS and NSA for advice and comment.

DEFINITIONS - See Appendix A.

BACKGROUND

Requirements of the Act

The Act establishes two basic requirements for Federal agencies relating to computer security plans:

> **Identification of Systems Containing Sensitive Information** - "[By July 8, 1988] each Federal agency shall identify each Federal computer system and system under development, which is within or under the supervision of that agency and which contains sensitive information."

> **Establishment of Security & Privacy Plans** - "[By January 8, 1989] each agency shall ... establish a plan for the security and privacy of each Federal computer system identified by that agency ... that is commensurate with the [sensitivity of] such system."

Such plans are to be "transmitted to NBS and NSA for advice and comment", and summaries of these plans are to be included in the agencies' IRM 5-year plan submissions to OMB. Instructions for meeting the latter requirement will be provided at a later date.

------ DRAFT ------
Revised: May 25, 1988

Objectives of Security Plan Review Process

The security plan review process is designed to improve the security of Federal computer systems by helping to identify and assess:

- the nature and extent of sensitive information systems in Government agencies and the security requirements of such systems;
- the adequacy of security planning and the basic administrative and technical approaches used by agencies in protecting sensitive systems;
- requirements for additional guidance, standards, assistance, training, and new technology to improve agencies' ability to protect sensitive and valuable information resources.

Effective security planning requires an analysis of system risks by identifying system assets, threats, and specific security vulnerabilities and assessing the presence and quality of specific controls. This can be done only by each agency, and it is not intended that the security plans submitted to NBS and NSA contain the details of such assessments. Rather, it is intended that each plan document the agency's own assessment of the security objectives of the system in question and the agency's plans to meet those objectives. It remains the agency's responsibility to evaluate specific risks and select appropriate, cost-effective security measures and to ensure that the security plan is effectively implemented.

APPLICABILITY

All Federal agencies are required to identify computer systems under their supervision containing sensitive information and to develop plans to ensure the security and privacy of such systems.

Contractor and Other Systems - The Act requires that agencies identify and prepare security plans for **all** sensitive Federal computer systems under their supervision. This includes contractor systems and systems operated by other organizations. Plans for such systems must be included as part of the agency's submission; they are not to be submitted separately.

The provisions of the Act and this guidance do not apply to systems containing classified information, systems involving intelligence activities, cryptologic activities related to national security, direct command and control of military forces, equipment that is integral to a weapons system or direct fulfillment of military or intelligence missions (excluded by U.S.C. 10-2315), or mixed classified/unclassified systems, provided such systems are always operated under rules for protecting classified information.

ACTION REQUIRED

Each agency must:

- By July 8, 1988 - identify systems under its supervision which contain sensitive information, and
- By January 8, 1989 - prepare security plans for each identified system and submit them to NBS and NSA for advice and comment.

Guidance for identifying systems and preparing the security plans is provided below and in the appendices.

IDENTIFICATION OF SYSTEMS CONTAINING SENSITIVE INFORMATION

Before agencies can develop security plans for systems containing sensitive information, they must identify such systems. The Act provides a working definition of "Sensitive Information". (See Appendix A.) It is the responsibility of each agency to apply this definition in the context of its own computer and telecommunications environment to determine which information is sensitive and to identify the systems which contain such information.

Identifying and Delineating Systems

The key to the security plan submission process lies in the identification and delineation of systems and each agency's identification of those systems containing data which is sensitive under the provisions of the Act. Agencies must draw the logical "boundaries" around such systems for planning and reporting purposes.

So that separate submissions do not have to be prepared for systems which have essentially the same function, characteristics, security needs, and security plans, agencies may, for the purpose of these submissions, treat two or more systems as a single system. Agencies will be required to indicate in their security plans which systems are actually a group of systems treated as one.

Agency management is expected to use its judgment in the identification and grouping of systems. It is not intended that agencies report separately on every minicomputer or smaller computer systems (or even every mainframe). However, it should also be clear that treating all of an agency's systems as a single generic group would be arbitrary and non-responsive to the Act.

Categories of Systems

For the purpose of reporting, systems should be grouped into two basic categories: 1) **Major Application Systems** and 2) **General ADP Support Systems** as described below.

Major Application Systems - These are systems that perform clearly defined functions and for which there are clearly identifiable security considerations and needs. Such a system might actually comprise many individual application programs and hardware, software, and telecommunications components. Examples might include a major agency benefits payment system, or a group of systems all supporting a specific agency program.

General ADP Support Systems - These consist of hardware and software that provide general ADP support for a variety of users and applications. Individual application systems are less easily distinguished than in the previous category but such applications may contain sensitive data. Even if none of the individual applications are sensitive, the support system itself could be considered sensitive if it provides critical support for the mission of the agency.

Several types of systems may be covered by this category. Examples include:

- an agency computer center, facility, or site
- an agency-wide data network
- a local area network
- a grouping of several personal computer workstations, perhaps connected by a local area network.

As indicated above, for each of the two system categories, agencies may treat two or more systems as a single system as long as they have essentially the same function, characteristics, security needs, and security plans.

FORMAT AND CONTENT OF SECURITY PLANS

Each system plan must include a basic description of the purpose, environment, and sensitivity of the system along with the security measures (in place or planned) intended to protect the system and its data. **These plans are not to be simply statements of agency security policy.** They should indicate security requirements and how the agency intends to meet those requirements.

Report Format

Agencies are requested to prepare their submissions in accordance with the specific organization and format described in Appendix B.

------ DRAFT ------
Revised: May 25, 1988

SUBMISSION OF MATERIALS

Submission Date

In accordance with the Act, Agency submissions should be received by January 8, 1989.

Submission Address

Two copies of the agency's submissions should be sent to the following address.

Computer Security Plan Review Team
National Bureau of Standards
Technology Building
Gaithersburg, MD 20899

INFORMATION CONTACTS

Questions regarding preparation or submission of the required reports should be directed to one of the following members of the review team:

Contacts to be Provided

------ DRAFT ------
Revised: May 25, 1988

APPENDIX A

DEFINITIONS

For the purposes of this guidance, the following definitions from the Act apply.

Computer System means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information. This includes:

- computers;
- ancillary equipment;
- software, firmware, and similar procedures;
- services, including support services; and
- related resources as defined by [the General Services Administration].

Federal Computer Systems means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function. This includes automatic data processing equipment as defined in the Federal Property and Administrative Services Act of 1949, as amended.

Operator of a Federal Computer System means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function.

Sensitive Information means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under [the Privacy Act], but which have not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Federal Agency is defined in section 3(b) of the Federal Property and Administrative Services Act of 1949, as amended.

------ DRAFT ------
Revised: May 25, 1988

APPENDIX B
INSTRUCTIONS FOR PREPARING SYSTEM SECURITY PLANS

GENERAL

The purpose of the agency security plan for each identified system is to provide a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. It is not intended to be a detailed technical description of system content, risks, or security mechanisms.

Each security plan should have four sections:

- o Basic System Identification and Description
- o Sensitivity of Data
- o Security and Privacy Measures
- o Needs and Additional Comments

The following is a description of the intended scope, content, and format of each section of the security plan.

------ DRAFT ------
Revised: May 25, 1988

1. BASIC SYSTEM IDENTIFICATION

Reporting Department or Agency

Organizational Subcomponent - Bureau or subagency

Operating Organization - The name of the organization responsible for direct operation or supervision of the system, if different from above. For example, this might be a contractor.

System Name/Title

System Category - Check one of the following:

[ ] Major Application
[ ] General-Purpose ADP Support System

Level of Aggregation - Indicate whether the identified system is a single identifiable element or a group of systems having sufficiently similar characteristics and security requirements as to be managed and reportable as a single system.

[ ] Single identifiable system
[ ] Group of similar systems

Operational Status - Indicate whether the identified system is currently in operation or is planned or under development.

[ ] Operational
[ ] Planned or Under Development

General Description/Purpose - A brief (1-2 paragraph) description of the function and purpose of the system.

System Environment and Special Considerations - A general description of the physical, operational, and technical environment in which the system operates. The physical location, types of computer hardware and software involved, types of users served, or other special considerations should be described.

Information Contact(s) - The name and telephone number of one or more persons designated to be the point-of-contact for this system. The designated persons should have sufficient knowledge of the system to be able to provide the review team with additional information, as needed.

2. SENSITIVITY OF SYSTEM OR DATA HANDLED

This section should provide an objective description of the types of data handled by the system. This should provide the basis for the system's security requirements.

General Description of Data or Systems Sensitivity - Describe, in general terms, of the nature of the data handled by the system and the need for protective measures.

Applicable Laws or Regulations Affecting the System - List any laws or regulations that establish specific requirements for protection of the system or its data. Examples might include the Privacy Act or a specific statute or regulation affecting information the agency processes (e.g., tax or census data). Note: This should **not** be a list of technical standards (e.g., FIPS 46) which determine how certain types of security mechanisms are to be implemented once the need for such protection has been determined. For similar reasons, the Computer Security Act of 1987 need not be listed.

System Protection Requirements - A system may need protection for one or more of the following reasons:

- **Confidentiality** - The system contains information that requires protection from unauthorized disclosure. Examples: For Official Use Only, timed or controlled dissemination (e.g., crop report data), personal data (covered by Privacy Act), confidential (proprietary) business information.

- **Integrity** - The system contains information which must be protected from unauthorized modification. Examples: Funds transfer systems.

- **Availability** - The system contains information or provides services which must be available on a timely basis to meet mission requirements. Example: Real-time monitoring or control systems.

A given system may contain several types of information, thus affecting the relative importance of each type of protection for that system. The purpose of this section is to indicate the type and relative importance of protection needed for the identified system. For each protection category, indicate if, for this system, the protection requirement is:

- P - Primary (i.e., the main security concern of the system)
- S - Secondary, or
- M - Minimal concern or not applicable

If needed, provide additional description of the data handled by the system and why the system requires the specified type(s) of protection.

Requires Confidentiality Protection [P] [S] [M]

Requires Integrity (Modification) Protection [P] [S] [M]

Requires Availability Protection/Assurance [P] [S] [M]

Risk Assessment - How were the risks and associated protection requirements for this system determined?

[ ] Formal Risk Analysis

[ ] Informal Risk Assessment(s)

[ ] Other (Describe)

Other Information - This should provide any additional information that will help describe the nature of the data handled by the systems and the protection requirements that have been identified for the information and the system.

3. SYSTEM SECURITY MEASURES

This section should describe the measures (in place or planned) that are intended to meet the protection requirements for the system. The types of protective measures should be consistent with the requirements described in the previous section.

Several basic categories of protective measures are outlined below. For each type of protective measure, the following information should be provided:

Status - An indication of the applicability or status of this type of control measure for the identified system:

[ ] **In Place** - Control measures of the type described are in place and operational, and judged to be effective. It is not necessary to decribe the details of the specific control measures.

[ ] **Planned** - Specific control measures (new, enhanced, etc.) are planned for the system. A general description of the planned measures and expected operational dates should be provided.

[ ] **Not applicable** - This type of control measure is not needed or appropriate for this system.

It should be noted that for an operational system, some specific controls of a given type may be "In Place" while others may be "Planned". For a system under development, it is to be expected that most measures will be "Planned".

Description of Planned Controls - This should be a brief description of the specific measures used (or planned) for this system.

Applicable Guidance - This should indicate the specific standards or other guidance (if any) used to design, implement, or operate the protective measures described. (e.g., relevant Federal or industry standards).

Comments - This should provide additional comments regarding the status, effectiveness, or special needs for this type of protection in the system.

The following pages list several general categories of control that should be in place for different types of systems. Although the basic categories are the same for all systems, there are some differences depending on the basic category of the identified system as described in the first section of the plan (i.e., Application System versus General ADP Support System). Therefore, this section of the security plan will follow either of two basic formats as described below.

APPLICATION SYSTEM CONTROLS

	In Place	Planned	N/A
MANAGEMENT CONTROLS			
Assignment of Responsibility	[ ]	[ ]	[ ]
Risk/Sensitivity Assessment	[ ]	[ ]	[ ]
Personnel Selection/Screening	[ ]	[ ]	[ ]
DEVELOPMENT CONTROLS			
Security Specifications	[ ]	[ ]	[ ]
Design Review & Testing	[ ]	[ ]	[ ]
Certification/Accreditation	[ ]	[ ]	[ ]
OPERATIONAL CONTROLS			
Production, I/O Controls	[ ]	[ ]	[ ]
Contingency Planning	[ ]	[ ]	[ ]
Audit & Variance Detection	[ ]	[ ]	[ ]
Software Maintenance Controls	[ ]	[ ]	[ ]
Documentation	[ ]	[ ]	[ ]
SECURITY AWARENESS & TRAINING			
Security Training & Awareness Measures	[ ]	[ ]	[ ]
TECHNICAL CONTROLS			
User Identification & Authentication	[ ]	[ ]	[ ]
Authorization/Access Controls	[ ]	[ ]	[ ]
Data Integrity/Validation Controls	[ ]	[ ]	[ ]
Journaling	[ ]	[ ]	[ ]
Transaction Journals			
Audit Trails			
Encryption	[ ]	[ ]	[ ]
INSTALLATION/FACILITY SECURITY MEASURES			
Security Measures for Supporting Facilities	[ ]	[ ]	[ ]
OTHER (DESCRIBE)			
____	[ ]	[ ]	[ ]

Description and Planned Operational Dates for Planned Measures

GENERAL ADP SUPPORT SYSTEM CONTROLS

	In Place	Planned	N/A
MANAGEMENT CONTROLS			
Assignment of Responsibility	[ ]	[ ]	[ ]
Risk Assessment	[ ]	[ ]	[ ]
Personnel Selection/Screening	[ ]	[ ]	[ ]
DEVELOPMENT/INSTALLATION			
Acquisition Specifications	[ ]	[ ]	[ ]
Certification/Accreditation	[ ]	[ ]	[ ]
OPERATIONAL CONTROLS			
Physical & Environmental Protection	[ ]	[ ]	[ ]
Production, I/O Controls	[ ]	[ ]	[ ]
Emergency, Backup & Contingency Plans	[ ]	[ ]	[ ]
Audit & Variance Detection	[ ]	[ ]	[ ]
System Software Controls	[ ]	[ ]	[ ]
Documentation	[ ]	[ ]	[ ]
SECURITY AWARENESS & TRAINING			
Security Training & Awareness Measures	[ ]	[ ]	[ ]
TECHNICAL CONTROLS			
User Identification & Authentication	[ ]	[ ]	[ ]
Authorization/Access Control	[ ]	[ ]	[ ]
Audit Trail Mechanisms	[ ]	[ ]	[ ]
Confidentiality Controls (e.g., encryption)	[ ]	[ ]	[ ]
Integrity Controls (e.g., message authentication)	[ ]	[ ]	[ ]
Other Technical (O/S) Security Mechanisms	[ ]	[ ]	[ ]
APPLICATION SYSTEM CONTROLS			
______________________________	[ ]	[ ]	[ ]
OTHER (Describe)	[ ]	[ ]	[ ]

Description and Planned Operational Dates for Planned Measures